John J. Nelson (SBN 317598)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
280 S. Beverly Drive
Beverly Hills, CA 90212
Telephone: (858) 209-6941
Fax: (858) 209-6941
Email: jnelson@milberg.com

Attorney for Plaintiff and the Proposed Class

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

NANCY ZIDE, individually and on behalf of all others similarly situated, Plaintiff, vs. SOVOS COMPLIANCE, LLC and PACIFIC PREMIER BANK, Defendants.	Case No. 8:23-cv-1711 Judge _____ CLASS ACTION JURY TRIAL DEMANDED

Plaintiff Nancy Zide ("Plaintiff") brings this Class Action Complaint ("Complaint") against Defendants Sovos Compliance, LLC and Pacific Premier Bank ("Defendants") as an individual and on behalf of all others similarly situated, and alleges, upon personal knowledge as to her own actions and her counsels' investigation, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. This class action arises out of the recent cyberattack and data breach ("Data Breach") resulting from Defendants' failure to implement reasonable and industry standard data security practices.

2. Defendant Sovos Compliance, LLC is a "global company" that provides regulatory and compliance services to its clients.

3. Defendant Pacific Premier Bank is a California-based bank that serves "businesses and individuals throughout the United States[,]" and boasts "approximately $21 billion in total assets[.]"[1]

4. In order to obtain financial services and/or other services at Defendants, Defendants require that customers and other personnel entrust Defendants with sensitive, non-public PII, without which Defendants could not perform their regular business activities. Defendants retain this information for at least many years.

5. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiff and Class Members, Defendants assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

[1] https://www.ppbi.com/about-us.html (last accessed Sep. 13, 2023).

6. On or about May 31, 2023, Defendants learned that one of their IT vendor's networks (Progress Software) had been penetrated by a cyberattack.[2] In response, Defendants launched an investigation and concluded—on an undisclosed date—that "unauthorized actors exploited the then-unknown MOVEit vulnerability to download a file containing some of [Plaintiff's and Class Members'] personal information."[3]

7. According to the Notice of Data Breach letter sent by Defendant Sovos Compliance, LLC to Plaintiff and other victims of the Data Breach (the "Notice Letter"), the compromised PII included individuals' full names, dates of birth, driver's license numbers, Pacific Premier account numbers, and Social Security numbers.[4]

8. Defendants failed to adequately protect Plaintiff's and Class Members PII—and failed to even encrypt or redact this highly sensitive information. This unencrypted, unredacted PII was compromised due to Defendants' negligent and/or careless acts and omissions and their utter failure to protect consumers' sensitive data. Hackers targeted and obtained Plaintiff's and Class Members' PII because of

[2] The "Notice Letter". A sample copy is available at https://apps.web.maine.gov/online/aeviewer/ME/40/761ef309-bd27-4146-b486-a2a540562e10.shtml (last accessed Sep. 13, 2023).

[3] *Id.*

[4] *Id.*

its value in exploiting and stealing the identities of Plaintiff and Class Members. The present and continuing risk to victims of the Data Breach will remain for their respective lifetimes.

9. Plaintiff brings this action on behalf of all persons whose PII was compromised as a result of Defendants' failure to: (i) adequately protect the PII of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of Defendants' inadequate information security practices; and (iii) effectively secure hardware containing protected PII using reasonable and effective security procedures free of vulnerabilities and incidents. Defendants' conduct amounts at least to negligence and violates federal and state statutes.

10. Defendants disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to implement and maintain adequate and reasonable measures and ensure those measures were followed by its IT vendors to ensure that the PII of Plaintiff and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party. Plaintiff and Class Members have a

continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

11. Plaintiff and Class Members have suffered injury as a result of Defendants' conduct. These injuries include: (i) invasion of privacy; (ii) theft of PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; and (vii) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

12. Plaintiff and Class Members seek to remedy these harms and prevent any future data compromise on behalf of herself and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach and who remain at risk due to Defendants' inadequate data security practices.

PARTIES

13. Plaintiff, Nancy Zide, is a natural person and citizen of Indio, California.

14. Defendant Sovos Compliance, LLC is a limited liability company

organized under the state laws of Delaware with its principal place of business located at 200 Ballardvale Street, 4th Floor, Wilmington, Massachusetts 01887.

15. Defendant Pacific Premier Bank is a bank organized under the state laws of California with its principal place of business located at 17901 Von Karman Avenue, Suite 1200, Irvine, California 92614.

JURISDICTION AND VENUE

16. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendants.[5]

17. This Court has personal jurisdiction over Defendants because Defendant Pacific Premier Bank's principal place of business is in this District, Defendants regularly conducts business in California and this District, and the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this District.

18. Venue is proper under 18 U.S.C § 1391(b)(1) because Defendant Pacific Premier Bank's principal place of business is in this District.

[5] According to the breach report submitted to the Office of the Maine Attorney General, 66 Maine residents were impacted in the data breach. *See* https://apps.web.maine.gov/online/aeviewer/ME/40/761ef309-bd27-4146-b486-a2a540562e10.shtml (last accessed Sep. 13, 2023).

FACTUAL ALLEGATIONS

Defendants' Businesses

19. Defendant Sovos Compliance, LLC is a "global company" that provides regulatory and compliance services to its clients.

20. Defendant Pacific Premier Bank is a California-based bank that serves "businesses and individuals throughout the United States[,]" and boasts "approximately $21 billion in total assets[.]"[6]

21. The information held by Defendants in their computer systems or those of its vendors at the time of the Data Breach included the unencrypted PII of Plaintiff and Class Members.

22. Upon information and belief, Defendants made promises and representations that the PII collected at Defendants would be kept safe, confidential, that the privacy of that information would be maintained, and that Defendants would delete any sensitive information after it was no longer required to maintain it.

23. Indeed, Defendant Sovos Compliance LLC's Privacy Policy provides that: "Sovos shall take reasonable steps to protect the Information from loss, misuse and unauthorized access, disclosure, alteration and destruction. Sovos has put in place appropriate physical, electronic and managerial procedures to safeguard and

[6] https://www.ppbi.com/about-us.html (last accessed Sep. 13, 2023).

secure the Information from loss, misuse, unauthorized access or disclosure, alteration or destruction."[7]

24. Moreover, Defendant Pacific Premier Bank's Privacy Policy provides that: "[w]e restrict access to nonpublic personal information about you to those employees who have a need to know such information (e.g., to process your transactions or provide services to you). We maintain physical, electronic, and procedural safeguards that comply with federal standards to guard your nonpublic personal information."[8]

25. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII. Plaintiff and Class Members relied on the sophistication of Defendants to keep their PII confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members value the confidentiality of their PII and demand security to safeguard their PII.

26. Defendants had a duty to adopt reasonable measures to protect the PII of Plaintiff and Class Members from involuntary disclosure to third parties and to audit, monitor, and verify the integrity of its IT vendors and affiliates. Defendants have a legal duty to keep consumer's PII safe and confidential.

[7] https://sovos.com/privacy-policy/ (last accessed Sep. 13, 2023).

[8] https://www.ppbi.com/lp/online-privacy-policy.html (last accessed Sep. 13, 2023).

27. Defendants had obligations created by FTC Act, the Gramm-Leach-Bliley Act, contract, industry standards, and representations made to Plaintiff and Class Members, to keep their PII confidential and to protect it from unauthorized access and disclosure.

28. Defendants derived a substantial economic benefit from collecting Plaintiff's and Class Members' PII. Without the PII, Defendants could not perform the services they provide.

29. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Defendants assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII from disclosure.

The Data Breach

30. On or about August 25, 2023, Defendant Sovos Compliance, LLC began sending the Notice of Data Breach letters (the "Notice Letter") to Plaintiff and Class Members, informing them that:

> **What happened?**
>
> MOVEit Transfer is a popular file transfer software used by government agencies, financial firms, universities, and other major organizations around the world. We utilize MOVEit to help deliver certain tax and regulatory compliance services to Pacific Premier Bank in relation to one or more accounts or payments belonging to you. On May 31, 2023, Progress Software, the owner of MOVEit, announced a previously unknown (i.e., zero-day) vulnerability in its MOVEit Transfer application. When we became aware of this incident, we immediately took the affected application

> offline and activated our incident response procedures. Outside advisors and cybersecurity experts were retained to assist in the evaluation of the situation, and we notified law enforcement. We recently determined that unauthorized actors exploited the then-unknown MOVEit vulnerability to download a file containing some of your personal information.
>
> **What information was involved?**
>
> The unauthorized third party downloaded a data file that may have contained your name, address, date of birth, social security number, driver's license number, and/or Pacific Premier account number.[9]

31. Omitted from the Notice Letter were the dates of the Data Breach, the details of the dates of Defendants' investigation; any explanation as to why Defendants failed to inform Plaintiff and Class Members of the Data Breach's occurrence for approximately three months after being informed by Progress Software of the Data Breach's occurrence, the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these omitted details have not been explained or clarified to Plaintiff and Class Members, who retain a vested interest in ensuring that their PII remains protected.

32. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiff and Class Members of the Data Breach's critical facts. Without these details, Plaintiff's and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

[9] Notice Letter.

33. Defendants did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiff and Class Members, causing the exposure of PII, such as encrypting the information or deleting it when it is no longer needed. Moreover, Defendants failed to exercise due diligence in selecting its IT vendors or deciding with whom it would share sensitive PII.

34. The attacker accessed and acquired files Defendants shared with a third party containing unencrypted PII of Plaintiff and Class Members, including their Social Security numbers and other sensitive information. Plaintiff's and Class Members' PII was accessed and stolen in the Data Breach.

35. Plaintiff further believes her PII and that of Class Members was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

Defendants Knew or Should Have Known of the Risk Because Financial Institutions and Regulatory Compliance Companies In Possession Of PII Are Particularly Suspectable To Cyber Attacks

36. Defendants' data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting financial institutions and/or regulatory compliance companies that collect and store PII, like Defendants, preceding the date of the breach.

37. Data breaches, including those perpetrated against financial

institutions and/or regulatory compliance companies that store PII in their systems, have become widespread.

38. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[10]

39. In light of recent high profile cybersecurity incidents at other healthcare partner and provider companies, including American Medical Collection Agency (25 million consumers, March 2019), University of Washington Medicine (974,000 consumers, December 2018), Florida Orthopedic Institute (640,000 consumers, July 2020), Wolverine Solutions Group (600,000 consumers, September 2018), Oregon Department of Human Services (645,000 consumers, March 2019), Elite Emergency Physicians (550,000 consumers, June 2020), Magellan Health (365,000 consumers, April 2020), and BJC Health System (286,876 consumers, March 2020), Defendants knew or should have known that its electronic records would be targeted by cybercriminals.

40. Indeed, cyber-attacks, such as the one experienced by Defendants, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and

[10] *See* 2021 Data Breach Annual Report (ITRC, Jan. 2022) (available at https://notified.idtheftcenter.org/s/), at 6.

prepared for, a potential attack. As one report explained, smaller entities that store PII are "attractive to ransomware criminals…because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[11]

41. Defendants knew and understood unprotected or exposed PII in the custody of healthcare entities, like Defendants, is valuable and highly sought after by nefarious third parties seeking to illegally monetize that PII through unauthorized access.

42. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members and of the foreseeable consequences that would occur if Defendants' data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

43. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

44. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendants' failure to implement or maintain adequate data

[11] https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection (last accessed Oct. 17, 2022).

security measures for the PII of Plaintiff and Class Members.

45. The ramifications of Defendants' failure to keep secure the PII of Plaintiff and Class Members are long lasting and severe. Once PII is stolen—particularly Social Security numbers—fraudulent use of that information and damage to victims may continue for years.

46. As a financial institution and/or regulatory compliance company in custody of PII, Defendants knew, or should have known, the importance of safeguarding the PII of Plaintiff and Class Members, and of the foreseeable consequences if their data security systems, or those of a vendor, were breached. This includes the significant costs imposed on Plaintiff and Class Members as a result of a breach. Defendants failed, however, to take adequate cybersecurity measures to prevent the Data Breach.

Value Of Personally Identifiable Information

47. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[12] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or

[12] 17 C.F.R. § 248.201 (2013).

identification number, alien registration number, government passport number, employer or taxpayer identification number."[13]

48. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web.

49. Numerous sources cite dark web pricing for stolen identity credentials.[14] For example, PII can be sold at a price ranging from $40 to $200.[15] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[16]

50. PII can sell for as much as $363 per record according to the Infosec Institute.[17] PII is particularly valuable because criminals can use it to target victims with frauds and scams.

51. Identity thieves use stolen PII such as Social Security numbers for a

[13] *Id.*

[14] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited Oct. 17, 2022).

[15] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Oct. 17, 2022).

[16] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Oct. 217, 2022).

[17] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited May 7, 2023).

variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

52. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

53. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[18] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[19] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies

[18] *Identity Theft and Your Social Security Number*, Social Security Administration (2018). Available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited May 7, 2023).

[19] *Id.*

the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

54. Moreover, it is not an easy task to change or cancel a stolen Social Security number:

> An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[20]

55. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

56. Driver's license numbers are also incredibly valuable. "Hackers harvest license numbers because they're a very valuable piece of information. A driver's license can be a critical part of a fraudulent, synthetic identity – which go for about $1200 on the Dark Web. On its own, a forged license can sell for around $200."[21]

57. According to national credit bureau Experian:

---

[20] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited May 7, 2023).

[21] https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3e4755c38658 (last visited on Feb. 21, 2023).

> A driver's license is an identity thief's paradise. With that one card, someone knows your birthdate, address, and even your height, eye color, and signature. If someone gets your driver's license number, it is also concerning because it's connected to your vehicle registration and insurance policies, as well as records on file with the Department of Motor Vehicles, place of employment (that keep a copy of your driver's license on file), doctor's office, government agencies, and other entities. Having access to that one number can provide an identity thief with several pieces of information they want to know about you. Next to your Social Security number, your driver's license number is one of the most important pieces of information to keep safe from thieves.

58. According to cybersecurity specialty publication CPO Magazine, "[t]o those unfamiliar with the world of fraud, driver's license numbers might seem like a relatively harmless piece of information to lose if it happens in isolation."[22] However, this is not the case. As cybersecurity experts point out:

> "It's a gold mine for hackers. With a driver's license number, bad actors can manufacture fake IDs, slotting in the number for any form that requires ID verification, or use the information to craft curated social engineering phishing attacks."[23]

59. Victims of driver's license number theft also often suffer unemployment benefit fraud, as described in a recent New York Times article.[24]

60. The fraudulent activity resulting from the Data Breach may not come

---

[22] https://www.cpomagazine.com/cyber-security/geico-data-breach-leaks-drivers-license-numbers-advises-customers-to-watch-out-for-fraudulent-unemployment-claims/ (last visited on Feb. 21, 2023).

[23] *Id.*

[24] *How Identity Thieves Took My Wife for a Ride,* NY Times, April 27, 2021, available at: https://www.nytimes.com/2021/04/27/your-money/identity-theft-auto-insurance.html (last visited on Feb. 21, 2023).

to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[25]

61. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[26]

62. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach

[25] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last visited Oct. 17, 2022).

[26] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited May 7, 2023).

is impossible to "close" and difficult, if not impossible, to change—names, dates of birth, and Social Security numbers.

Defendants Fail To Comply With FTC Guidelines

63. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

64. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal consumer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[27]

65. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan

[27] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Oct. 17, 2022).

ready in the event of a breach.[28]

66. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

67. The FTC has brought enforcement actions against financial institutions and regulatory compliance companies for failing to protect consumer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

68. These FTC enforcement actions include actions against financial institutions and regulatory compliance companies, like Defendants.

69. Defendants failed to properly implement basic data security practices.

70. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers' PII constitutes an unfair act or

[28] *Id.*

practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

71. Upon information and belief, Defendants were at all times fully aware of its obligation to protect the PII of its consumers and other personnel in its network. Defendants were also aware of the significant repercussions that would result from its failure to do so.

Pacific Bank Fails To Comply with the Gramm-Leach-Bliley Act

72. Defendant Pacific Bank is a financial institution, as that term is defined by Section 509(3)(A) of the Gramm-Leach-Bliley Act ("GLBA"), 15 U.S.C. § 6809(3)(A), and thus are subject to the GLBA.

73. The GLBA defines a financial institution as "any institution the business of which is engaging in financial activities as described in Section 1843(k) of Title 12 [The Bank Holding Company Act of 1956]." 15 U.S.C. § 6809(3)(A).

74. Pacific Bank collects nonpublic personal information, as defined by 15 U.S.C. § 6809(4)(A), 16 C.F.R. § 313.3(n) and 12 C.F.R. § 1016.3(p)(1). Accordingly, during the relevant time period Pacific Bank was subject to the requirements of the GLBA, 15 U.S.C. §§ 6801.1, *et seq*., and is subject to numerous rules and regulations promulgated on the GLBA statutes.

75. The GLBA Privacy Rule became effective on July 1, 2001. *See* 16 C.F.R. Part 313. Since the enactment of the Dodd-Frank Act on July 21, 2010, the CFPB became responsible for implementing the Privacy Rule. In December 2011,

the CFPB restated the implementing regulations in an interim final rule that established the Privacy of Consumer Financial Information, Regulation P, 12 C.F.R. § 1016 ("Regulation P"), with the final version becoming effective on October 28, 2014.

76. Accordingly, Pacific Bank's conduct is governed by the Privacy Rule prior to December 30, 2011 and by Regulation P after that date.

77. Both the Privacy Rule and Regulation P require financial institutions to provide consumers with an initial and annual privacy notice. These privacy notices must be "clear and conspicuous." 16 C.F.R. §§ 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. "Clear and conspicuous means that a notice is reasonably understandable and designed to call attention to the nature and significance of the information in the notice." 16 C.F.R. § 313.3(b)(1); 12 C.F.R. § 1016.3(b)(1). These privacy notices must "accurately reflect[] [the financial institution's] privacy policies and practices." 16 C.F.R. § 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. They must include specified elements, including the categories of nonpublic personal information the financial institution collects and discloses, the categories of third parties to whom the financial institution discloses the information, and the financial institution's security and confidentiality policies and practices for nonpublic personal information. 16 C.F.R. § 313.6; 12 C.F.R. § 1016.6. These privacy notices must be provided "so that each consumer can

reasonably be expected to receive actual notice." 16 C.F.R. § 313.9; 12 C.F.R. § 1016.9. As alleged herein, Pacific Bank violated the Privacy Rule and Regulation P.

78. Upon information and belief, Pacific Bank failed to provide annual privacy notices to consumers after the consumer relationship ended, despite retaining these consumers' PII and storing that PII on Pacific Bank's network systems.

79. Pacific Bank failed to adequately inform consumers that they were storing and/or sharing, or would store and/or share, the consumers' PII on an insecure platform, accessible to unauthorized parties from the internet, and would do so after the consumer relationship ended.

80. The Safeguards Rule, which implements Section 501(b) of the GLBA, 15 U.S.C. § 6801(b), requires financial institutions to protect the security, confidentiality, and integrity of consumer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards, including: (1) designating one or more employees to coordinate the information security program; (2) identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of consumer information, and assessing the sufficiency of any safeguards in place to control those risks; (3) designing and implementing

information safeguards to control the risks identified through risk assessment, and regularly testing or otherwise monitoring the effectiveness of the safeguards' key controls, systems, and procedures; (4) overseeing service providers and requiring them by contract to protect the security and confidentiality of consumer information; and (5) evaluating and adjusting the information security program in light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances. 16 C.F.R. §§ 314.3 and 314.4.

81. As alleged herein, Pacific Bank violated the Safeguard Rule.

82. Pacific Bank failed to assess reasonably foreseeable risks to the security, confidentiality, and integrity of consumer information and failed to monitor the systems of its IT partners or verify the integrity of those systems.

83. Pacific Bank violated the GLBA and their own policies and procedures by sharing the PII of Plaintiff and Class Members with a non-affiliated third party without providing Plaintiff and Class Members (a) an opt-out notice and (b) a reasonable opportunity to opt out of such disclosure.

Defendants Fail To Comply With Industry Standards

84. As noted above, experts studying cyber security routinely identify entities in possession of PII as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

85. Several best practices have been identified that, at a minimum, should

be implemented by financial institutions and/or regulatory compliance companies in possession of PII, like Defendants, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Defendants failed to follow these industry best practices, including a failure to implement multi-factor authentication.

86. Other best cybersecurity practices that are standard in the financial services and regulatory compliance industries include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. Defendants failed to follow these cybersecurity best practices, including failure to train staff.

87. Defendants failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security

Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

88. These foregoing frameworks are existing and applicable industry standards in the financial services and regulatory compliance industries, and upon information and belief, Defendants failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

Defendants Breached their Duty to Safeguard Consumers' PII

89. In addition to its obligations under federal and state laws, Defendants owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendants owed a duty to Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the PII of Class Members

90. Defendants breached their obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data and failed to audit, monitor, or ensure the integrity of its vendor's data security practices. Defendants' unlawful conduct

includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;

b. Failing to adequately protect consumers' PII;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to audit, monitor, or ensure the integrity of its vendor's data security practices;

e. Failing to sufficiently train its employees and vendors regarding the proper handling of its consumers PII;

f. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;

g. Failing to adhere to the Gramm-Leach-Bliley Act and industry standards for cybersecurity as discussed above; and,

h. Otherwise breaching duties and obligations to protect Plaintiff's and Class Members' PII.

91. Defendants negligently and unlawfully failed to safeguard Plaintiff's and Class Members' PII by allowing cyberthieves to access its computer network and systems which contained unsecured and unencrypted PII.

92. Had Defendants remedied the deficiencies in its information storage

and security systems or those of its vendors and affiliates, followed industry guidelines, and adopted security measures recommended by experts in the field, it could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiff's and Class Members' confidential PII.

COMMON INJURIES & DAMAGES

93. As a result of Defendants' ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of PII ending up in the possession of criminals, the risk of identity theft to the Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (c) the loss of benefit of the bargain (price premium damages); (d) diminution of value of their PII; I invasion of privacy; and (f) the continued risk to their PII, which remains in the possession of Defendants, and which is subject to further breaches, so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII.

The Data Breach Increases Victims' Risk Of Identity Theft

94. Plaintiff and Class Members are at a heightened risk of identity theft for years to come.

95. The unencrypted PII of Class Members will end up for sale on the dark

web because that is the *modus operandi* of hackers. In addition, unencrypted PII may fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the PII of Plaintiff and Class Members.

96. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal PII to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

97. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity--or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

98. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data Breaches can be the starting point

for these additional targeted attacks on the victim.

99. One such example of criminals piecing together bits and pieces of compromised PII for profit is the development of "Fullz" packages.[29]

100. With "Fullz" packages, cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

101. The development of "Fullz" packages means here that the stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff' and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a

[29] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-](https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/ (last visited on May 26, 2023).

higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

102. The existence and prevalence of "Fullz" packages means that the PII stolen from the data breach can easily be linked to the unregulated data (like phone numbers and emails) of Plaintiff and the other Class Members.

103. Thus, even if certain information (such as emails or telephone numbers) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package.

104. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

Loss Of Time To Mitigate Risk Of Identity Theft And Fraud

105. As a result of the recognized risk of identity theft, when a Data Breach occurs, and an individual is notified by a company that their PII was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet, the resource and asset of time has been lost.

106. Thus, due to the actual and imminent risk of identity theft, Plaintiff

and Class Members must, as Defendants' Notice Letter encourages, monitor their financial accounts for many years to mitigate the risk of identity theft.

107. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as changing passwords and resecuring their own computer networks, contacting credit bureaus to ensure their accounts are secure, and researching and verifying the legitimacy of the Data Breach.

108. Plaintiff's mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[30]

109. Plaintiff's mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze

[30] *See* United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), https://www.gao.gov/new.items/d07737.pdf.

on their credit, and correcting their credit reports.[31]

110. And for those Class Members who experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[32]

Diminution Value Of PII

111. PII is a valuable property right.[33] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

112. An active and robust legitimate marketplace for PII exists. In 2019, the data brokering industry was worth roughly $200 billion.[34]

---

[31] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps (last visited July 7, 2022).

[32] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (last visited Sep. 13, 2022) ("GAO Report").

[33] *See, e.g.,* Randall T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[34] https://www.latimes.com/business/story/2019-11-05/column-data-brokers

113. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[35,36]

114. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[37]

115. Conversely sensitive PII can sell for as much as $363 per record on the dark web according to the Infosec Institute.[38]

116. As a result of the Data Breach, Plaintiff's and Class Members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the PII is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

117. Based on the foregoing, the information compromised in the Data

[35] https://datacoup.com/

[36] https://digi.me/what-is-digime/

[37] Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at https://computermobilepanel.nielsen.com/ui/US/en/faqen.html

[38] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited Sep. 13, 2022).

Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change, e.g., names, Social Security numbers, and dates of birth.

118. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

119. The fraudulent activity resulting from the Data Breach may not come to light for years.

120. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members, and of the foreseeable consequences that would occur if Defendants' data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

121. Defendants were, or should have been, fully aware of the unique type and the significant volume of data on Defendants' networks, amounting to over two hundred thousands individuals' detailed personal information, upon information and belief, and thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

122. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

Future Cost of Credit and Identity Theft Monitoring is Reasonable and Necessary

123. Given the type of targeted attack in this case and sophisticated criminal activity, the type of PII involved, and the volume of data obtained in the Data Breach, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the PII for identity theft crimes –*e.g.,* opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

124. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

125. Furthermore, the information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, where victims can easily cancel or close credit

and debit card accounts.[39] The information disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

126. Consequently, Plaintiff and Class Members are at a present and continuous risk of fraud and identity theft for many years into the future.

127. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from Defendants' Data Breach. This is a future cost for a minimum of five years that Plaintiff and Class Members would not need to bear but for Defendants' failure to safeguard their PII.

PLAINTIFF ZIDE'S EXPERIENCE

128. Plaintiff Nancy Zide does not know how Defendants obtained her PII and was not familiar with Defendants prior to receiving the Notice Letter from Defendant Sovos Compliance, LLC.

129. Upon information and belief, at the time of the Data Breach, Defendants retained Plaintiff's PII in their system, despite Plaintiff not being a customer at Defendants.

[39] *See* Jesse Damiani, *Your Social Security Number Costs $4 On The Dark Web, New Report Finds*, FORBES (Mar. 25, 2020), https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1.

130. Plaintiff Nancy Zide is very careful about sharing her sensitive PII. Plaintiff stores any documents containing her PII in a safe and secure location. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff would not have allowed Defendants to maintain her PII had she known of Defendants' lax data security policies.

131. Plaintiff Nancy Zide received the Notice Letter, by U.S. mail, directly from Defendant Sovos Compliance, LLC, dated August 25, 2023. According to the Notice Letter, Plaintiff's PII was improperly accessed and obtained by unauthorized third parties, including her name, date of birth, driver's license number, and Social Security number.

132. As a result of the Data Breach, and at the direction of Defendants' Notice Letter, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including changing passwords and resecuring her own computer networks, contacting credit bureaus to ensure her accounts are secure, and researching and verifying the legitimacy of the Data Breach. Plaintiff has spent significant time dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

133. Plaintiff suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii)

theft of PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; and (vii) the continued and certainly increased risk to her PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

134. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed her of key details about the Data Breach's occurrence.

135. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

136. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

137. Plaintiff Nancy Zide has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

138. This action is properly maintainable as a class action. Plaintiff brings this class action on behalf of herself and on behalf of all others similarly situated.

139. Plaintiff proposes the following Class definitions, subject to amendment as appropriate:

Nationwide Class
All individuals residing in the United States whose PII was compromised in the data breach announced by Defendants in August 2023 (the "Class").

California Subclass
All individuals residing in the state of California whose PII was compromised in the data breach announced by Defendants in August 2023 (the "California Subclass").

140. Excluded from the Classes are the following individuals and/or entities: Defendants and Defendants' parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendants has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

141. Numerosity: The members of the Class are so numerous that joinder of all members is impracticable, if not completely impossible. At least 215,000 individuals were notified by Defendants of the Data Breach, according to the breach

report submitted to Office of the Maine Attorney General.[40] The Class is apparently identifiable within Defendants' records, and Defendants have already identified these individuals (as evidenced by sending them breach notification letters).

142. Common questions of law and fact exist as to all members of the Class that predominate over any questions affecting solely individual members of the Class. The questions of law and fact common to the Class, which may affect individual Class members, include, but are not limited to, the following:

a. Whether and to what extent Defendants had a duty to protect the PII of Plaintiff and Class Members;

b. Whether Defendants had respective duties not to disclose the PII of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendants had respective duties not to use the PII of Plaintiff and Class Members for non-business purposes;

d. Whether Defendants failed to adequately safeguard the PII of Plaintiff and Class Members;

e. Whether and when Defendants actually learned of the Data Breach;

f. Whether Defendants adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;

[40] *See* https://apps.web.maine.gov/online/aeviewer/ME/40/761ef309-bd27-4146-b486-a2a540562e10.shtml (last accessed Sep. 13, 2023).

g.. Whether Defendants violated the law by failing to promptly notify Plaintiff and Class Members that their PII had been compromised;

h. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Plaintiff and Class Members are entitled to actual damages, statutory damages, and/or nominal damages as a result of Defendants' wrongful conduct; and

k. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

143. Typicality: Plaintiff's claims are typical of those of the other members of the Class because Plaintiff, like every other Class Member, was exposed to virtually identical conduct and now suffers from the same violations of the law as each other member of the Class.

144. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendants acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of

uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Nationwide Class as a whole. Defendants' policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendants' conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

145. Adequacy: Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that she has no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiff seeks no relief that is antagonistic or adverse to the Class Members and the infringement of the rights and the damages she has suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex class action and data breach litigation, and Plaintiff intends to prosecute this action vigorously.

146. Superiority and Manageability: The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit

the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendants. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

147. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendants would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

148. The litigation of the claims brought herein is manageable. Defendants' uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

149. Adequate notice can be given to Class Members directly using information maintained in Defendants' records.

150. Unless a Class-wide injunction is issued, Defendants may continue in their failure to properly secure the PII of Class Members, Defendants may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendants may continue to act unlawfully as set forth in this Complaint.

151. Further, Defendants have acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Code of Civil Procedure § 382.

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

152. Plaintiff restates and realleges the preceding factual allegations set forth above as if fully alleged herein.

153. Plaintiff and the Class entrusted Defendants with their PII, directly or indirectly, on the premise and with the understanding that Defendants would safeguard their information, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

154. Defendants had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Class could and would suffer if the PII were wrongfully

disclosed.

155. By collecting and storing this data on Defendants' computer system and network, and sharing it and using it for commercial gain, Defendants owed a duty of care to use reasonable means to secure and safeguard their computer system—and Class Members' PII held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendants' duty included a responsibility to implement processes by which it could detect a breach of their security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

156. Defendants owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected the PII.

157. Defendants' duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendants and the individuals who entrusted them with PII, which is recognized by laws and regulations, as well as common law. Defendants were in a superior position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

158. Defendants' duty to use reasonable security measures required

Defendants to reasonably protect confidential data from any intentional or unintentional use or disclosure. In addition, Defendants had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

159. Pacific Bank's duty to use reasonable security measures also arose under the GLBA, under which they were required to protect the security, confidentiality, and integrity of consumer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards.

160. Defendants' duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendants are bound by industry standards to protect confidential PII.

161. Defendants breached their duties, and thus were negligent, by failing to use reasonable measures to protect Class Members' PII. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;

b. Failing to adequately monitor the security of their networks and systems;

c. Failing to have in place mitigation policies and procedures;

d. Failing to audit, monitor, or ensure the integrity of its vendor's data security practices;

e. Allowing unauthorized access to Class Members' PII;

f. Failing to detect in a timely manner that Class Members' PII had been compromised; and,

g. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

162. Defendants owed to Plaintiff and Class Members a duty to notify them within a reasonable timeframe of any breach to the security of their PII. Defendants also owed a duty to timely and accurately disclose to Plaintiff and Class Members the scope, nature, and occurrence of the data breach. This duty is required and necessary for Plaintiff and Class Members to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the data breach.

163. Defendants breached their duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security

practices to safeguard Plaintiff's and Class Members' PII.

164. Defendants further breached their duties by failing to provide reasonably timely notice of the data breach to Plaintiff and Class Members, which actually and proximately caused and exacerbated the harm from the data breach and Plaintiff and Class Members' injuries-in-fact.

165. Defendants owed these duties to Plaintiff and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendants knew or should have known would suffer injury-in-fact from Defendants' inadequate security protocols.

166. Defendants violated Section 5 of the FTC Act and GLBA by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

167. Plaintiff and Class Members were within the class of persons the Federal Trade Commission Act and GLBA were intended to protect and the type of harm that resulted from the Data Breach was the type of harm these statues were intended to guard against.

168. Defendants' violation of Section 5 of the FTC Act and GLBA

constitutes negligence.

169. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

170. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendants' inadequate security practices.

171. It was foreseeable that Defendants' failure to use reasonable measures to protect Class Members' PII would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the financial services and regulatory compliance industries.

172. Defendants had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Class could and would suffer if the PII were wrongfully disclosed.

173. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendants knew or should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Class, the critical importance of providing adequate security of that PII, and the necessity

for encrypting PII stored on Defendants' systems.

174. It was therefore foreseeable that the failure to adequately safeguard Class Members' PII would result in one or more types of injuries to Class Members.

175. Defendants were in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

176. Defendants' duty extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

177. Defendants have admitted that the PII of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

178. But for Defendants' wrongful and negligent breach of duties owed to Plaintiff and the Class, the PII of Plaintiff and the Class would not have been compromised.

179. There is a close causal connection between Defendants' failure to implement security measures to protect the PII of Plaintiff and the Class and the

harm, or risk of imminent harm, suffered by Plaintiff and the Class. The PII of Plaintiff and the Class was lost and accessed as the proximate result of Defendants' failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

180. As a direct and proximate result of Defendants' negligence, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; and (vii) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant’s possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

181. As a direct and proximate result of Defendants' negligence, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

182. Additionally, as a direct and proximate result of Defendants'

negligence, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII in its continued possession.

183. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

184. Defendants' negligent conduct is ongoing, in that Defendants still hold the PII of Plaintiff and Class Members in an unsafe and insecure manner.

185. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendants to (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II
Unjust Enrichment / Quasi Contract
(On Behalf of Plaintiff and the Class)

186. Plaintiff restates and realleges the preceding factual allegations set forth above as if fully alleged herein.

187. Plaintiff and Class Members conferred a monetary benefit on Defendants. Specifically, they provided Defendants with their PII. In exchange, Plaintiff and Class Members should had their PII protected with adequate data

security.

188. Defendants knew that Plaintiff and Class Members conferred a benefit upon it and has accepted and retained that benefit by accepting and retaining the PII entrusted to it. Defendants profited from Plaintiff's retained data and used Plaintiff's and Class Members' PII for business purposes.

189. Defendants failed to secure Plaintiff's and Class Members' PII and, therefore, did not fully compensate Plaintiff or Class Members for the value that their PII provided.

190. Defendants acquired the PII through inequitable record retention as it failed to disclose the inadequate data security practices previously alleged.

191. If Plaintiff and Class Members had known that Defendants would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and secure their PII, they would have entrusted their PII at Defendants or obtained services at Defendants.

192. Plaintiff and Class Members have no adequate remedy at law.

193. Under the circumstances, it would be unjust for Defendants to be permitted to retain any of the benefits that Plaintiff and Class Members conferred upon it.

194. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i)

invasion of privacy; (ii) theft of PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; and (vii) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

195. Plaintiff and Class Members are entitled to full refunds, restitution, and/or damages from Defendants and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendants from its wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiff and Class Members may seek restitution or compensation.

196. Plaintiff and Class Members may not have an adequate remedy at law against Defendants, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT III
Violations of California's Unfair Competition Law ("UCL")
Unlawful Business Practice
Cal Bus. & Prof. Code § 17200, *et seq.*
(On Behalf of Plaintiff and the California Subclass)

197. Plaintiff restates and realleges all proceeding allegations above and hereafter as if fully set forth herein and brings this claim individually and on behalf of the proposed the California Subclass (the "Class" for the purposes of this Count).

198. By reason of the conduct alleged herein, Defendants engaged in unfair and unlawful "business practices" within the meaning the meaning of California's Unfair Competition Law ("UCL"), Business and Professions Code § 17200, *et seq.*

199. Defendants stored the PII of Plaintiff and the Class Members in its computer systems and knew or should have known it did not employ reasonable, industry standard, and appropriate security measures that complied with federal regulations and that would have kept Plaintiff's and the Class Members' PII a secure and prevented the loss or misuse of that PII.

200. Plaintiff and Class Members were entitled to assume, and did assume, Defendants would take appropriate measures to keep their PII safe.

201. Defendants did not disclose at any time that Plaintiff's PII was vulnerable to hackers because Defendants' data security measures were inadequate and outdated, and Defendants were the only entities in possession of that material information, which it had a duty to disclose.

202. Defendants violated the UCL by failing to maintain the safety of its computer systems, specifically the security thereof, and its ability to safely store Plaintiff's and Class Members' PII.

203. Defendants violated the UCL by failing to implement reasonable and appropriate security measures or follow industry standards for data security, failing to comply with its own posted privacy policies, and by failing to immediately timely and adequately notify Plaintiff and Class Members of the Data Breach.

204. Section 5 of the FTCA required Defendants to take reasonable measures to protect Plaintiff's and the Class Member's PII data and is a further source of Defendants' duty to Plaintiff and the Class Members.

205. Section 5 prohibits unfair practices in or affecting commerce, including, as interpreted and enforced by the FTC, the unfair act or practice by businesses like Defendants of failing to implement and use reasonable measures to protect Sensitive Information. Defendant, therefore, was required and obligated to take reasonable measures to protect PII it solicited, possessed, held, or otherwise used. The FTC publications and data security breach orders described herein further form the basis of Defendants' duty to adequately protect Sensitive Information. By failing to implement and use reasonable data security measures, Defendants acted in violation of § 5 of the FTCA.

206. Defendants' acts, omissions, and misrepresentations as alleged herein were unlawful and in violation of, *inter alia*, Section 5(a) of the Federal Trade Commission Act.

207. If Defendants had complied with these legal requirements, Plaintiff and

Class Members would not have suffered the damages related to the Data Breach, and consequently from, Defendants' failure to timely notify Plaintiff and the Class Members of the Data Breach.

208. Moreover, Defendants' collection of sensitive consumers' PII in combination with its failure to implement reasonable security safeguards demonstrate Defendants' violation of the unfair prong of the UCL.

209. Defendants violated the unfair prong of the UCL by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting Plaintiff's and Class Members' PII with knowledge that the information would not be adequately protected; and by storing Plaintiff's and Class Members' PII in an unsecure electronic environment. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiff and Class Members. They were likely to deceive the public into believing their PII was securely stored when it was not. The harm these practices caused to Plaintiff and Class Members outweighed their utility, if any.

210. Plaintiff and Class Members have lost money and property as a result of Defendants' violations of the UCL as they were denied the benefit of their transacting with Defendants because Defendants failed to use funds from money paid by Plaintiff and Class Members to supply adequate data security.

211. Moreover, Plaintiff and Class Members, directly or indirectly, provided

their PII to Defendant, which is property as defined by the UCL, and their property has been diminished in value as a result of the loss of its confidentiality.

212. Plaintiff and Class Members have also suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*, (i) invasion of privacy; (ii) theft of PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; and (vii) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

213. Unless restrained and enjoined, Defendants will continue to engage in the above-described wrongful conduct and more data breaches will occur.

214. As such, Plaintiff, on behalf of herself and Class Members, seeks restitution and an injunction, including public injunctive relief prohibiting Defendants from continuing such wrongful conduct, and requiring Defendants to modify their corporate cultures and design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls,

policies, procedures protocols, and software and hardware systems to safeguard and protect the PII entrusted to it, as well as all other relief the Court deems appropriate, consistent with Bus. & Prof. Code § 17203.

215. To the extent any of these remedies are equitable, Plaintiff and the Class seek such equitable remedies, in the alternative to any adequate remedy at law they may have.

COUNT IV
Violations of the California Consumer Privacy Act of 2018 ("CCPA")
Cal. Civ. Code § 1798, *et seq.*
(On Behalf of Plaintiff and the California Subclass)

216. Plaintiff restates and realleges all proceeding allegations above and hereafter as if fully set forth herein and brings this claim individually and on behalf of the proposed the California Subclass (the "Class" for the purposes of this Count).

217. As more personal information about consumers is collected by businesses, consumers' ability to properly protect and safeguard their privacy has decreased. Consumers entrust businesses with their personal information on the understanding that businesses will adequately protect it from unauthorized access and disclosure.

218. The California Legislature explained: "The unauthorized disclosure of personal information and the loss of privacy can have devasting effects for individuals, ranging from financial fraud, identity theft, and unnecessary costs to personal time and finances, to destruction of property, harassment, reputational

damage, emotional stress, and even potential physical harm."[41]

219. As a result, in 2018, the California Legislature passed the CCPA, giving consumers broad protections and rights intended to safeguard their personal information. Among other things, the CCPA imposes an affirmative duty on businesses that maintain personal information about California residents to implement and maintain reasonable security procedures and practices that are appropriate to the nature of the information collected.

220. Defendants failed to implement such procedures which resulted in the Data Breach.

221. CCPA also requires "[a] business that discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party . . . [to] require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." Cal. Civ. Code § 1798.81.5(c).

222. Section 1798.150(a)(1) of the CCPA provides: "Any consumer whose nonencrypted or nonredacted personal information, as defined [by the CCPA] is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of

[41] California Consumer Privacy Act (CCPA) Compliance, https://buyergenomics.com/ccpa-complience/

the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for" statutory or actual damages, injunctive or declaratory relief, and any other relief the court deems proper.

223. Plaintiff and the Class Members are "consumer[s]" as defined by Civ. Code § 1798.140(g) because they are "natural person[s] who [are] California resident[s], as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017."

224. Defendants are both "business[es]" as defined by Civ. Code § 1798.140(c) because Defendant:

a. is a "sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners";

b. "collects consumers' personal information, or on the behalf of which is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information";

c. does business in California; and

d. has annual gross revenues in excess of $25 million; annually buys, receives for the business' commercial purposes, sells or shares for

commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices; or derives 50 percent or more of its annual revenues from selling consumers' personal information.

225. The PII taken in the Data Breach is personal information as defined by Civil Code § 1798.81.5(d)(1)(A) because it contains Plaintiff's and the Class members' unencrypted first and last names and Social Security numbers, among other information.

226. Plaintiff's and the Class's PII was subject to unauthorized access and exfiltration, theft, or disclosure because their PII, including name and Social Security numbers, was wrongfully taken, accessed, and viewed by unauthorized third parties.

227. The Data Breach occurred as a result of Defendants' failure to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect Plaintiff's and the Class members' PII. Defendants failed to implement reasonable security procedures to prevent an attack on their server or network, including its email system, by hackers and to prevent unauthorized access of Plaintiff's and Class Members' PII as a result of this attack.

228. On September 14, 2023, Plaintiff provided Defendants with written notice of their violations of the CCPA, pursuant to Civil Code § 1798.150(b)(1), asserting violations of Civil Code §§ 1798.81.5 and 1798.150.

229. If Defendants have not cured or are unable to cure the violations described therein within thirty days of receipt, Plaintiff will amend her complaint to seek all relief available under the CCPA including damages to be measured as the greater of actual damages or statutory damages in an amount up to seven hundred and fifty dollars ($750) per consumer per incident. See Cal. Civ. Code § 1798.150(a)(1)(A) & (b).

230. As a result of Defendants' failure to implement and maintain reasonable security procedures and practices that resulted in the Data Breach, Plaintiff seeks injunctive relief, including public injunctive relief and declaratory relief.

COUNT V
Invasion of Privacy
Cal. Const. Art. 1 § 1
(On Behalf of Plaintiff and the California Subclass)

231. Plaintiff restates and realleges all proceeding allegations above and hereafter as if fully set forth herein and brings this claim individually and on behalf of the proposed the California Subclass (the "Class" for the purposes of this Count).

232. California established the right to privacy in Article I, Section 1 of the California Constitution.

233. Plaintiff and the Class had a legitimate expectation of privacy to their PII and were entitled to the protection of this information against disclosure to unauthorized third parties.

234. Defendants owed a duty to Plaintiff and the Class to keep their PII

contained confidential.

235. Defendants failed to protect and released to unknown and unauthorized third parties the PII and of Plaintiff and the Class.

236. Defendants allowed unauthorized and unknown third parties access to and examination of the PII of Plaintiff and the Class, by way of Defendants' failure to protect the PII.

237. The unauthorized release to, custody of, and examination by unauthorized third parties of the PII of Plaintiff and the Class is highly offensive to a reasonable person.

238. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and the Class disclosed their PII to Defendants, directly or indirectly, with an intention that the PII would be kept confidential and would be protected from unauthorized disclosure. Plaintiff and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

239. The Data Breach at the hands of Defendants constitutes an intentional interference with Plaintiff's and the Class's interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

240. Defendants acted with a knowing state of mind when they permitted the

Data Breach to occur because they were with actual knowledge that its information security practices were inadequate and insufficient.

241. Because Defendants acted with this knowing state of mind, they had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiff and the Class.

242. As a proximate result of the above acts and omissions of Defendant, the PII of Plaintiff and the Class was disclosed to third parties without authorization, causing Plaintiff and the Class to suffer damages.

243. Unless and until enjoined, and restrained by order of this Court, Defendants' wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class in that the PII and maintained by Defendants can be viewed, distributed, and used by unauthorized persons for years to come.

244. Plaintiff and the Class have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and the Class.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

A. For an Order certifying this action as a class action and appointing Plaintiff and her counsel to represent the Class and California Subclass;

B. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PII, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

C. For equitable relief compelling Defendants to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII compromised during the Data Breach;

D. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. Prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

ii. Requiring Defendants to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

iii. Requiring Defendants to delete, destroy, and purge the PII of Plaintiff and Class Members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. Requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;

v. Prohibiting Defendants from maintaining the PII of Plaintiff and Class Members on a cloud-based database;

vi. Requiring Defendants to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

vii. Requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. Requiring Defendants to audit, test, and train its security personnel regarding any new or modified procedures;

ix. Requiring Defendants to segment data by, among other things, creating firewalls and access controls so that if one area of Defendants' network is compromised, hackers cannot gain access to other portions of Defendants' systems;

x. Requiring Defendants to conduct regular database scanning and securing checks;

xi. Requiring Defendants to establish an information security training program that includes at least annual information security training for all consumers, with additional training to be provided as appropriate based upon the consumers' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xii. Requiring Defendants to routinely and continually conduct internal training and education, and on an annual basis to

inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. Requiring Defendants to implement a system of tests to assess its respective consumers' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing consumers' compliance with Defendants' policies, programs, and systems for protecting personal identifying information;

xiv. Requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. Requiring Defendants to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves; and

xvi. Requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendants' servers; and

xvii. for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendants' compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the Class, and to report any deficiencies with compliance of the Court's final judgment.

E. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendants' wrongful conduct;

F. Ordering Defendants to pay for not less than ten years of credit monitoring services for Plaintiff and the Class;

G. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

H. For an award of punitive damages, as allowable by law;

I. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

J. Pre- and post-judgment interest on any amounts awarded; and

K. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury on all claims so triable.

Dated: September 14, 2023

Respectfully submitted,

s/ John J. Nelson

John J. Nelson (SBN 317598)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
280 S. Beverly Drive
Beverly Hills, CA 90212
Telephone: (858) 209-6941
Fax: (858) 209-6941
Email: jnelson@milberg.com

Attorney for Plaintiff and the Proposed Class